JMMB Financial Holdings Limited
Anti-Money Laundering, Counter Terrorist Financing, and Counter Proliferation Financing Policy

---

Date of Board Audit & Compliance Approval: August 24, 2023

Date of Board of Directors ratification

Effective Date
Original issue date: Sept 28 , 2023

Next Scheduled Review Date
Revision Date: September 2024 ; (Policies should be reviewed at a minimum of once every year)

Table of Contents

List of Abbreviations

Terms	Definitions
AML/CTF/CPF	Anti-Money Laundering/Counter Terrorist Financing/Counter Proliferation Financing
KYC	Know Your Customer
KYE	Know Your Employee
EDD	Enhanced Due Diligence
CDD	Client Due Diligence
PEP	Politically Exposed Person
BOJ	Bank of Jamaica
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
JMMB GL / JMMB Group / Group	JMMB Group Limited
FHL	JMMB Financial Holdings Limited
ML	Money Laundering
TF	Terrorist Financing
PF	Proliferation Financing
GCCO	Group Chief Compliance Officer
RGO	Regional Governance Officer
BACC	Board Audit & Compliance Committee
CCO	Country Compliance Officer

Policy Definitions

For ease of reference, please note the following terms used throughout this Policy:

- "FHL Group" refers to the entirety of the JMMB Financial Holdings Limited (FHL), including its wholly owned subsidiaries and their branches regardless of geographical location.
- "JMMB Group" refers to the parent company of JMMB Financial Holdings Limited.
- "Financial Subsidiaries" refers to the financial entities wholly owned by the FHL regardless of geographic location.
- "Regulator[1]" refers to the regulatory body with supervisory and licencing authority over a Financial Subsidiary.
- "Designated Authority" refers to the local or national agency, authority or department which has oversight over Anti-Money Laundering (AML)/Counter Terrorist Financing (CTF)/Counter Proliferation Financing (CPF) and reporting related thereto in the respective jurisdiction in which a Financial Subsidiary is located.
- "Responsible Officer[2]" refers to the officer in charge of AML/CTF/CPF compliance for a Financial Subsidiary.
- "Red flag" refers to a warning signal that should bring attention to a potentially suspicious activity, situation or transaction.
- "Typologies" refers to the various techniques, methods or schemes that are used for money laundering and other financial crimes.
- "Contractors" refers to persons who are contracted to the FHL or its subsidiaries in the capacity of team members but are working on a contractual basis.

[1] Jurisdictional nomenclature may include Competent Authorities, Central Banks, Securities and Exchange Commissions, Financial Services Authorities

[2] Jurisdictional nomenclature may include Compliance Officer, Chief Compliance Officer, Nominated Officer

1. Introduction

1.1. Background

JMMB Financial Holdings Limited (FHL) was established to be the parent company all of the regulated financial entities (Financial Subsidiaries) of JMMB Group Limited (JMMBGL) and is subject to the regulatory oversight of the Bank of Jamaica (BOJ). The FHL exercises direct oversight of all Financial Subsidiaries.

The FHL Board of Directors has ownership of this Policy and has delegated the responsibility for the oversight of anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) matters to the Board of Directors for each Financial Subsidiary.

1.2. Policy Scope

This policy is applicable to the FHL, its Financial Subsidiaries and their branches regardless of geographical location, and extends to all business lines, transactions and activities, products and services offered. This Policy applies to the members of the FHL and its Financial Subsidiaries inclusive of Boards of Directors, team leaders, team members, contractors, consultants and other third parties to whom we may outsource our functions.

1.3. Policy Statement

Sound risk management practices with respect to AML/CTF/CPF recommend that regional or international groups operating in multiple jurisdictions should develop a group-wide AML/CTF/CPF policy to ensure an effective oversight for risk across their regional or international operations. The FHL Group is committed to conducting business in conformity with legal, ethical and professional standards and understands its role in combating Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF). Against this background, the FHL Group has adopted a consolidated approach to the establishment and implementation of its AML/CTF/CPF policies and procedures.

1.4. Policy Purpose

This Policy is prepared for application to the FHL, its Financial Subsidiaries and their branches, and is designed to:

i) Outline the minimum compliance requirements with the legal and regulatory frameworks across the FHL Group and international best practice around AML/CTF/CPF;
ii) Protect the reputation and integrity of the FHL Group by implementing adequate controls and systems to prevent the possibility of the Group's people, products and services being used for ML/TF/PF;
iii) Ensure that Directors, team leaders, team members, consultants and contractors are aware of and understand AML/CTF/CPF and their responsibilities as they pertain to the same;
iv) Ensure that team members are able to:
    a) recognize ML/TF/PF activity,
    b) identify and report all suspicious transactions, and
    c) clearly understand the implications of non-compliance;

v) Standardise as far as possible, a group-wide approach to AML/CTF/CPF risk management, client due diligence, on-boarding and on-going monitoring, identification and reporting of unusual/suspicious activity, know your employee, record retention and facilitate the on-going training of Directors and team members.

1.5. Application of the Policy

This Policy represents the minimum standards by which the FHL, Financial Subsidiaries and their branches, irrespective of geographical location and jurisdiction, are governed with respect to AML/CTF/CPF. Each Financial Subsidiary is required to assess the existing AML/CTF/CPF regime in the jurisdiction in which it operates to ensure it applies the requirement of the Jamaican law. Where the AML/CTF/CPF requirements in other jurisdictions are stricter than the Jamaican requirements, the Financial Subsidiaries operating in those respective jurisdictions should ensure that additional measures are developed and implemented to adequately meet the standards in the overseas jurisdictions.

In this regard, supporting procedures at the country and subsidiary levels may vary as they are required to also reflect local requirements and business line considerations. To this end, each geographical territory must develop an AML/CTF/CPF manual with the detailed operational guidelines applicable to their respective jurisdiction. The country specific manuals should be read in conjunction with this FHL Policy in order to obtain a detailed understanding of the AML/CTF/CPF programme for each Financial Subsidiary.

Where regulators in the respective locations specifically require it, a Financial Subsidiary shall adopt their own AML/CTF/CPF policy, but the same should be in line with this Policy and should be subject to the ratification of the FHL's Board.

1.6. Relationship to Other Policies and Procedures

This FHL policy should be used in conjunction with the following policies, manuals, guidelines:

- Country Specific AML/CTF/CPF Manuals
- JMMB FHL Client and Account Management Guidelines
- JMMB Group People Policy
- JMMB Group Anti-Bribery and Corruption Policy
- JMMB FHL Enterprise Compliance Framework
- JMMB FHL Enterprise Risk Management Policy
- JMMB Group Data Protection and Privacy Policy
- JMMB Group Ethics and Code of Conduct Policy

2. Overview of Money Laundering, Terrorist Financing And Proliferation Financing

2.1. Money Laundering – Definition and the Three Stages

Money Laundering (ML) is the process used by criminals to conceal the illegal origin and ownership of money derived from criminal activities. If successfully undertaken, it allows criminals to maintain control over those proceeds until the money loses their criminal identity and appear to have been legitimately derived.

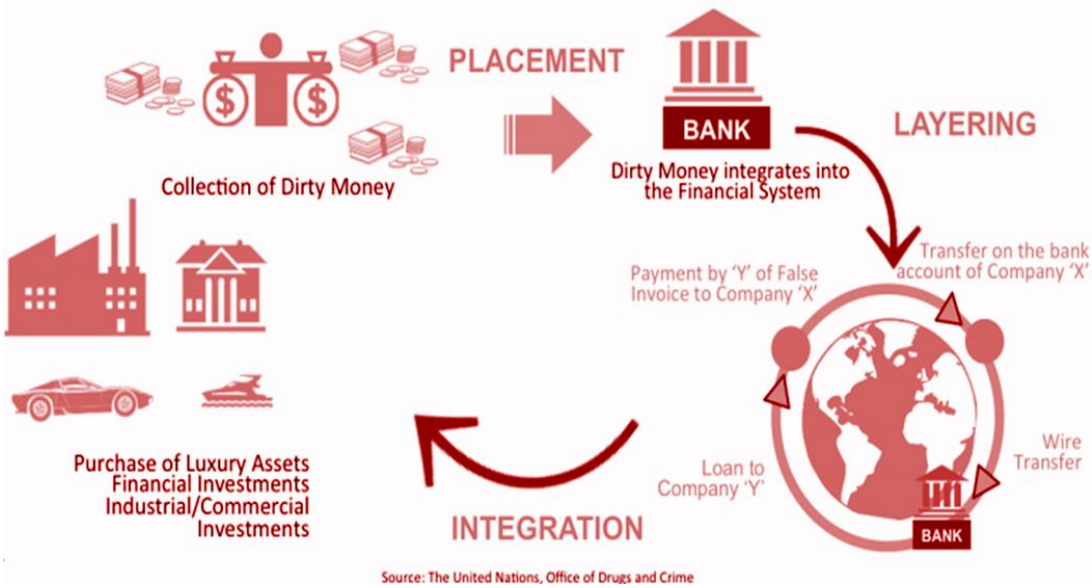
Crimes that are specific to ML are referred to as "Predicate Offenses" or "predicate crimes". Law-giving and law enforcement bodies worldwide are continuously expanding the criminal activities that are regarded as Predicate Offenses. These include but are not limited to:

- Tax Evasion
- Corruption
- Fraud
- Human and Wildlife trafficking
- Forgery
- Narcotics trafficking

The ML process involves three (3) main stages, namely, placement, layering and integration, defined as follows:

i. **Placement**: After getting hold of illegally acquired funds through the commission of a Predicate Offence, criminals move the cash from its source. This is where the criminal money is "washed" and disguised by being placed into the legitimate financial system without arousing suspicion, for example via deposits, purchases of cheques or money orders;
ii. **Layering**: The "Layering" stage is used to disguise the criminal origin of illegal funds. Layering activities can include using multiple banks and accounts, having professionals act as intermediaries, and layers of complex financial transactions sometimes across multiple jurisdictions. The goal is to disguise the paper trail or audit trail of the funds and anonymize the criminals' activity and identity. These transactions may include purchasing investment instruments, insurance contracts, wire transfers, money orders and letters of credit; and
iii. **Integration**: Refers to the attempt to legitimise wealth derived from criminal activity. The illicit funds re-enter the legitimate economy by way of investment in real estate, luxury assets and business ventures until the laundered funds are eventually dispersed back to the criminal through the formal system appearing to be legitimate funds. At this stage, it is very difficult to distinguish between legal and illegal wealth. It is extremely challenging to catch the criminal if there is no documentation to use as evidence from the previous stages and therefore the importance of closely observing the Know Your Customer (KYC) guidelines.

Figure 1 Model Money Laundering Scheme



2.2. Terrorism Financing

Terrorism is the unlawful threat of action designed to compel the government or an international organisation, or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause.

Terrorists and terrorist organisations need funding to sustain themselves and carry out terrorist acts. Terrorism Financing is the process by which funds are provided to an individual or group to finance terrorist acts. It involves the provision of funds directly or indirectly, intending or knowing that the funds are to be used to fund terrorist acts or organisations. It encompasses the means and methods used by terrorist organisations to finance activities that threaten national and international security.

Money can come from legitimate sources including profits from businesses and charitable organisations and criminal sources such as drug trade, weapon smuggling or kidnapping for ransom.

Modern day terrorists are now leaning toward the use of modern technologies, including the block-chain and cryptocurrencies. In today's environment, cryptocurrency is being heavily used to help fund attacks more easily than fiat currency allows.

Terrorists often use public officials who abuse the authority of their public office for personal gain. Students, non-profit organisations and schools are often used as conduits for the movement of funds as they give the appearance of validity.

If a Terrorism Financing scheme is successful, funds are typically used to:

- Increase and maintain the functioning of the terrorist organisation.
- Provide basic technical necessities.
- Cover costs related to the spreading of terrorist ideologies.

- Fund the training of perpetrators of actual acts of terrorism.

2.3. Proliferation Financing

Proliferation of Weapons of Mass Destruction (WMD) is the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes) in contravention of national laws or international obligations. It includes technology, goods, software, services or expertise.

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the proliferation of WMD.

Proliferation financing can be achieved through:

- Terrorism Financing where it provides financial support to terrorist organisations that want to acquire and/or use WMD; or
- Financing from a state or a state-controlled or state-sponsored entity with the aim of acquiring new or enhanced WMD.

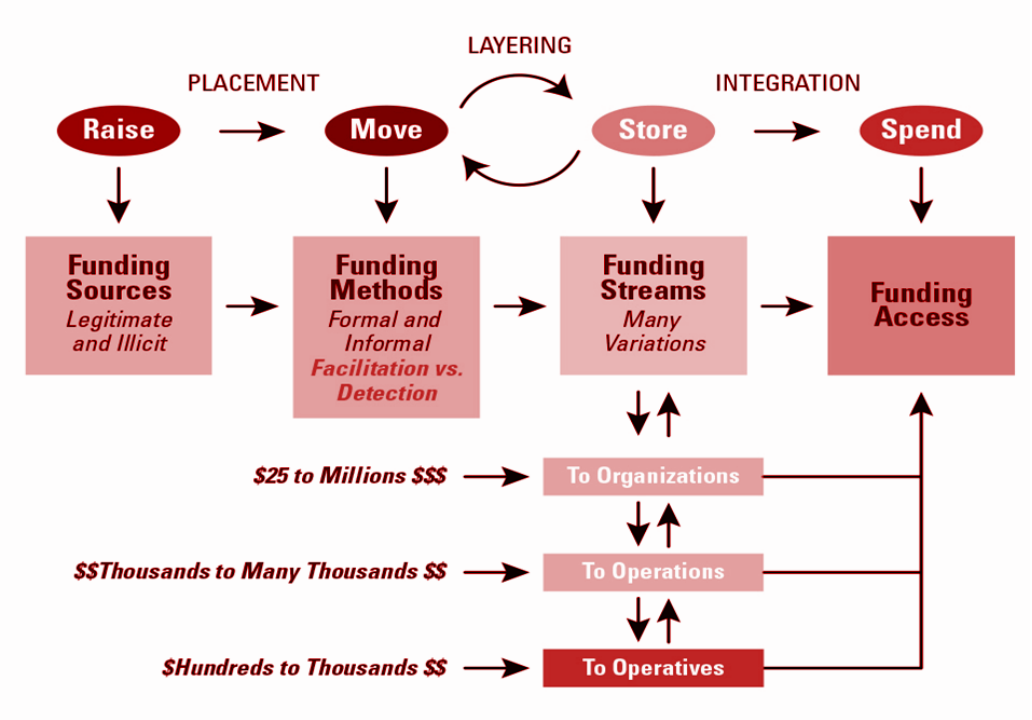
2.4. Terrorism and Proliferation Financing – the Four Stages

Stage 1 – Raising: The generating of funds intended for Terrorist and Proliferation Financing. This may include legitimate businesses, direct donations by individuals and organisations, the use of charities and non-profit organisations and criminal activity.

Stages 2 and 3 – Moving and Storing: These stages may be interchanged and can be compared to the Layering stage in Money Laundering. The financial sector, smuggling and cryptocurrencies are all used to move and store funds.

Stage 4 – Spending: Stored funds are spent on weapons, material, equipment, media, messaging, training and to cover salaries, living expenses and travel costs for terrorist fighters.

Figure 2 Model Terrorism/Proliferation Financing Scheme



3. Governance Framework

3.1. Roles and Responsibilities

In order to comply with AML/CTF/CPF requirements, various officers within the FHL Group have assigned roles and responsibilities which are vital to the implementation of an effective AML/CTF/CPF risk management framework. The ultimate responsibility for compliance with AML/CTF/CPF policies and procedures resides with the respective Boards of Directors who should have a clear understanding of the ML/TF/PF risks faced by the Financial Subsidiaries and the risk framework in place to mitigate risks identified.

See *Appendix 16.1* for details of the Governance roles and responsibilities for the administration of AML/CTF/CPF risk framework for the FHL Group.

3.2. Information Sharing across the Group

In order to facilitate effective monitoring and good governance, the Board of Directors of FHL has approved the sharing of information among the Financial Subsidiaries of the Group with respect to client and transaction information when necessary for the purposes of AML/CTF/CPF, provided always that such information is maintained with the strictest of confidence and subject to data protection standards.

The Group Chief Compliance Officer (GCCO) is authorised to request, directly or through the Regional Governance Officer (RGO), and the Responsible Officers are required to proactively provide as needed:

i. Information concerning high-risk clients and activities; and
ii. Due diligence and transaction information on shared clients or where a client of one Financial Subsidiary is desirous of transacting or opening an account with another Financial Subsidiary.

This Section 3.2 is subject to the data protection and privacy laws and regulations applicable in each jurisdiction around the different types of information that may be shared within a financial group for AML/CTF/CPF purposes, and the requirements for storage, retrieval, sharing/distribution and disposal of this information.

The GCCO is further authorised to request, directly or through the RGO, that any Financial Subsidiary search their files against specified lists, or to request information on individuals or organisations suspected of aiding and abetting ML/TF/PF, and report matches to the relevant designated authority or take any action necessary to protect the FHL Group.

3.3. Information Sharing with Regulatory Authorities

Regulatory authorities of the FHL Group (e.g. the BOJ as the "super-regulator" for the FHL's home jurisdiction) are able to request access to the information it needs to verify group-wide compliance with this Policy and supporting procedures during on-site inspections. This may require review of client files and a sampling of accounts or transactions conducted by Financial Subsidiaries. This use of information for a legitimate supervisory need, safeguarded by the confidentiality provisions applicable to Regulators, is not impeded by local bank secrecy or data protection laws.

4. Legal and Regulatory Framework

In carrying out activities and transactions, Directors, team leaders and team members of the FHL, its Financial Subsidiaries and their branches should be aware of the AML/CTF/CPF laws, regulations, standards and guidelines along with their legal obligation and responsibilities as well as fines and penalties associated with offences as prescribed by the regulatory framework.

Directors, team leaders and team members should be mindful that the failure to comply with the legal and regulatory framework for AML/CTF/CPF could have serious implications for each individual as well as the FHL Group.

See *Appendix 16. 2* for a listing of the applicable laws, regulations and guidelines applicable to the Legal and Regulatory Framework for AML/CTF/CPF in the various territories in which the FHL Group operates. A summary of the AML/CTF/CPF applicable laws and regulations and the details of the relevant offences and associated penalties applicable to each jurisdiction should be included in each country specific AML/CTF/CPF manual.

In particular, and as a rule of general application, Directors, team leaders and team members of the FHL, its Financial Subsidiaries and their branches are required to understand the offences of "Tipping off" and "Wilful Blindness".

Tipping Off

Tipping Off occurs where a person knows or suspects that a disclosure has been made to the Responsible Officer, law enforcement or the Designated Authority, and they disclose to another person this information or any other matter which is likely to prejudice any investigation that might be conducted following the disclosure.

There is therefore a general prohibition on disclosing to the client the fact that a suspicious activity or related information was reported to the Responsible Officer or that an external report was made to the Designated Authority.

Wilful Blindness

Wilful Blindness is where a person fails to disclose knowledge or suspicion of ML/TF/PF. It occurs when a person ignores facts which a reasonable person would consider suspicious.

It is important to note that a person does not have to be actively involved in money laundering in order to be held legally liable for the crime of money laundering. To the contrary, if a person has direct knowledge or if they ought to have known that funds were tainted and they failed to investigate red flags for suspicious activity and still completes a transaction involving such funds, they may be liable for the offence of money laundering.

Even where there is no direct evidence of a person's knowledge concerning tainted funds, they may be found to have been wilfully blind or to have acted with reckless disregard for the facts, and therefore still be liable.

The directors, team leaders and team members of the FHL and its Financial Subsidiaries and their branches are therefore urged to report all matters that appear unusual or suspicious to the Responsible Officer for review and investigation.

Co-operation with Legislative and Regulatory Authorities

A critical component of the FHL Group's AML/CTF/CPF programme is the cooperation with relevant authorities and law enforcement bodies in the jurisdictions where the Financial Subsidiaries reside. Accordingly, the FHL commits to full cooperation with the Competent Authorities and the Designated Authorities in each jurisdiction for the purpose of fulfilling its obligations under the law. Orders served or requests made to the FHL or its Financial Subsidiaries by the relevant authorities are to be kept in the strictest confidence by all team members who become aware of such requests.

5. Risk Based Framework

5.1. Scope

The FHL Group has adopted a risk-based approach to combating ML/FT/PF and seeks to ensure that measures are in place to identify, assess and take effective mitigation actions proportionate with the

risks identified. This approach allows resources to be allocated in keeping with proprieties so that the greatest risks receive the highest attention.

5.2. Enterprise Risk Assessment and Reporting

In order to apply risk management principles, the FHL Group needs to be aware of the inherent ML/TF/PF risks which are present in its operations. As such, an Enterprise Risk Assessment of ML/TF/PF must be conducted, reviewed and updated in accordance with the regulatory requirements of each jurisdiction or at shorter intervals where there are material events. Material trigger events which could prompt earlier review include business expansion through mergers and acquisitions, the introduction of new products and services as a result of new and developing technologies or the decision to on-board high risk clients or groups of clients as a specific strategic initiative.

The risk assessment must be documented and approved by the FHL Board. The results of the assessment should be readily available to team leaders, internal auditors, external auditors and Regulators/Competent Authorities.

Specific financial subsidiary risk assessments must also be conducted in line with the regulatory requirements in each jurisdiction, and may be based on the material trigger events set out above and or/as prescribed by the applicable Regulator.

The risk assessment should be informed by relevant information from various sources such as national risk assessments, mutual evaluation reports and reports from law enforcement bodies. At a minimum, the following ML/TF/PF risk factors should be assessed:

a. Clients and other counterparts; parties (i.e. persons other than clients with whom Financial Subsidiaries conduct business);
b. countries or geographic areas;
c. products;
d. services;
e. transactions;
f. delivery channels; and
g. operating environment (business – size, activities and complexities; sector; regulatory frameworks and national and global issues).

5.3. Three Lines of Defence Model

The First Line of Defence

The FHL has aligned with the "Three Lines of Defence" Model. In this regard, Business Units (client-facing functions) constitute the first line of defence with responsibility for identifying, assessing, controlling, mitigating and reporting on the ML/FT/FP encountered in the course of business. They are required to adhere to risk limits, policy guidelines, and implement/use approved procedures set by the second line of defence. In the context of AML/CTF/CPF, the first line of defence is also required to identify unusual/suspicious activity in real time, as well as unusual behaviour exhibited by clients, and

to be vigilant in the identification, escalation and reporting of unusual/suspicious transactions and activity.

The Second Line of Defence

The Responsible Officer and the Compliance Team are part of the second line of defence, and are responsible for ongoing monitoring of compliance with AML/CTF/CPF requirements. This includes sample testing of KYC compliance and reviews of exception reports to alert team leaders or the Board of Directors of the FHL and its Financial Subsidiaries if it is believed management is failing to address AML/CTF/CPF procedures in a responsible manner.

The business interests of a Financial Subsidiary should in no way be opposed to the effective discharge of the duties of the Responsible Officer, and conflicts of interest must be avoided. Therefore, to enable unbiased judgments and facilitate impartial advice to management, the Responsible Officer should not have business line responsibilities and should not be entrusted with responsibilities in the areas of data protection or internal audit.

The Responsible Officer should be provided with sufficient resources to execute his/her responsibilities effectively, thereby playing a central and proactive role in the Financial Subsidiary's AML/CTF/CPF regime. In order to do so, he/she must be fully conversant with statutory and regulatory requirements and the ML/TF/PF risks arising from the business.

The Third Line of Defence

Internal Audit is charged with the third line of defence and is separate from both the first and second lines of defence. Internal Audit plays an important role in independently evaluating risk management and controls, and discharges its responsibility to the Board Audit and Compliance Committee (BACC) through periodic reviews of FHL's controls, processes and systems and the effectiveness of the compliance with AML/CTF/CPF policies and procedures.

Further, there are additional external levels of control that complement the above three (3) internal lines of control. External auditors and the Regulators play a critical role in independently assessing the overall governance and control structure to determine whether there is adequate compliance with the relevant standards and rules.

1. External auditors are required by law to conduct annual AML/CTF/CPF audits and submit their reports, which are shared with the Regulators in keeping with timelines specified for each jurisdiction.

2. Regulators issue guidance to regulated entities and also assess their compliance with regulatory rules and standards.

6. Required Procedures

6.1. Know Your Client, Client Acceptance and Identification Procedures

The FHL and its Financial Subsidiaries and their branches will not establish a business relationship until all relevant parties to the relationship have been satisfactorily identified, verified and the nature of the business they intend to conduct ascertained. The primary aim of this policy is to limit the risk of

the FHL and its Financial Subsidiaries being used to conduct ML/TF/PF and other criminal activities. In order to achieve this, FHL and its Financial Subsidiaries will employ a risk-based due diligence process which entails the collection and verification of information proportionate to the level of risks associated with each business relationship.

Each jurisdiction is required to implement its own Know Your Client, Client Acceptance and Identification Procedures. At a minimum, these procedures should:

i. Include a process for assessing a client's risk for ML/TF/PF. When assessing a client's risk, consideration should be given to factors such as the client's background, occupation, source of income and wealth, country of origin and residence (when different), products used, nature and purpose of accounts, linked accounts, business activities and other client-oriented risk indicators. These may include the intended purpose and nature of the account or transaction and expected level of activity.
ii. Include a process for the screening of clients against sanctions list(s) of known or suspected terrorists stipulated by the Designated Authority and adverse/negative media at on-boarding and on an on-going basis.
iii. Be risk-based, requiring standard client due diligence standard (CDD) in the majority of cases, with commensurate enhanced due diligence (EDD) as the level of risk associated with the client increases[3]. For proven lower risk situations, simplified due diligence (SDD) may be permitted, if this is allowed by law.
iv. Establish the baseline due diligence for categories of clients and based on client risk.
v. Not be so restrictive that it results in a denial of access by the general public to financial services, especially for clients who are financially or socially disadvantaged[4].
vi. Define circumstances under which the financial subsidiary would not accept a new business relationship or would terminate an existing one.
vii. Include a systematic procedure using reliable, independent source documents, data or information for identifying and verifying clients' identity and, where applicable, any person acting on a client's behalf, and any beneficial owner(s).
viii. Be comprehensive enough to allow for the building of a client's risk profile. This is critical as the client's risk profile is what facilitates the identification of any account activity that could be considered as unusual or suspicious or deviates from activity or behaviour that would be considered "normal" for the particular client or client category.

6.2. Reporting Procedures

The FHL and its Financial Subsidiaries will implement the relevant systems and procedures to identify and report any known or suspected ML/TF/PF activities to the Designated Authority. Each Financial Subsidiary is therefore required to implement its own procedures for internal and external reporting in keeping with the requirement of each jurisdiction and consistent with this FHL Policy.

Internal Reporting

[3] Enhanced due diligence may be essential for an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or an individual who is a politically exposed person (PEP). In particular, such enhanced due diligence is required for foreign PEPs. Decisions to enter into or pursue business relationships with high-risk clients should require the application of enhanced due diligence measures, such as approval to enter into or continue such relationships, being taken by team leaders.

[4] The FATF Financial Inclusion Guidance provides useful guidelines on designing AML/CTF.CPF procedures that are not overly restrictive to the financially or socially disadvantaged

The process for identifying, investigating and reporting suspicious transactions to the Responsible Officer should be clearly specified in the internal procedures and communicated to all team members through regular training. These procedures should contain a clear description for team members of their obligations and instructions for the analysis, investigation and reporting/escalation of such activity within the Financial Subsidiary, as well as guidance on how to complete such reports.

External Reporting

These procedures should set out the financial subsidiary's statutory obligations under recognised suspicious activity reporting regimes, cash threshold reporting, consent regime and other reporting/disclosure obligations to the Designated Authority. These procedures should also reflect the principle of confidentiality and ensure that investigations are conducted swiftly and that reports contain accurate and relevant information, and are produced and submitted in a timely manner.

These procedures should also present options available to the Responsible Officer where suspicion has been raised in relation to an account or relationship, including, in addition to reporting the suspicious activity, ensuring that appropriate action is taken to adequately mitigate the risk of the Financial Subsidiary being used for criminal activities. This may include a review of either the risk classification of the client, account or of the entire relationship itself. Appropriate action may necessitate escalation to the RGO or GCCO to determine how to handle the relationship, taking into account other relevant factors, such as cooperation with law enforcement agencies or other external bodies.

6.3. Sanction Screening/Asset Freezing Procedures

Each Financial Subsidiary is required to implement its own procedures for Sanction Screening/Asset Freezing in keeping with the requirement of each jurisdiction.

These procedures should specify that sanction screening is not a risk-sensitive due diligence measure and must be carried out regardless of the client's risk profile. At minimum, there should be a requirement for clients to be screened at on-boarding, and at regular intervals (based on the requirement for the jurisdiction) against the United Nations Security Council Consolidated List the U.S. and any jurisdictional Consolidated Lists issued by local regulators pertaining to persons/entities identified as terrorist or involved in terrorist activity (Designated Persons and Entities). The transaction screening process and the list management process should also be addressed in each country specific procedure.

These procedures should also cover the process to enforce asset freezing (and the removal of asset freezing) directives given by the Designated Authority and should specify the process for detecting transactions with Designated Persons and Entities. It should be specifically noted that terrorist screening is not a risk-sensitive due diligence measure and should be carried out, irrespective of the risk profile attributed to the client. Further, these procedures should specify the requirement to freeze, without delay and without prior notice, the funds or other assets of Designated Persons and Entities, and to file relevant reports to the Designated Authority in keeping with applicable laws and regulations in each jurisdiction.

6.4. Record and Retention

Each Financial Subsidiary is required to implement its own procedures for the management of information/records.

These procedures should at minimum:

i. Include a definition of the types of information and documentation that should be included in the financial subsidiary's records as well as the retention period for such records.
ii. Specify that even if accounts are closed, in the event of an ongoing investigation/litigation, all records should be retained until the closure of the case.
iii. Specify that records are stored in a manner that will allow the Financial Subsidiary to meet any requests of the Regulator or the Designated Authority based on prescribed requirements in the legal and regulatory framework.

6.5. Client and Account Management

Each Financial Subsidiary is required to adopt the FHL's Client and Account Management Guidelines, or where regulation requires, implement its own Client Account Management Procedures. At a minimum, these procedures should cover the requirements to on-board clients and periodic due diligence reviews to keep their information updated on an on-going basis, and should deal with the treatment of special classes of accounts, clients and situations.

6.6. Know Your Employee

The FHL Group recognizes that the ability to implement an effective AML/ CTF/CPF programme depends in part on the quality and integrity of team members. As such, each Financial Subsidiary is required to have procedures in place to undertake due diligence on prospective and existing team members throughout the course of employment.

These procedures should at minimum include:

i. Verification procedures for the applicant's identity and personal information, including employment history and background.
ii. a risk-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased for existing team members.
iii. appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or team member provided.
iv. ongoing monitoring of team members to ensure that they continue to meet the Group's standards of integrity, competence and compliance.
v. a process for on-going monitoring of team members' transactions.

7. Detection, Monitoring and Testing

7.1. Identification of Unusual/Suspicious Activity

Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis to determine if they are. Some indicators of unusual transactions are:

i. Where a transaction is inconsistent in amount, origin, destination or type with a client's known, legitimate business or personal activities;
ii. Complex transactions or structures which have no apparent economic or visible lawful purpose.

The following factors should be considered when determining whether a transaction may be suspicious or unusual:

i. Does the client have an established business relationship with the Financial Subsidiary?
ii. Is the transaction in keeping with the client's normal activity, the markets in which the client normally trades or the client's own business?
iii. Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market size and frequency?
iv. Is the role of any agent or any other individual involved in the transaction unusual?
v. Is the transaction to be settled in the normal manner?
vi. Are there any other transactions linked to the transaction in question which may appear to be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?
vii. Does the structure, nature and purpose of the transaction make sense? Might there be an easier, cheaper or more convenient method available? Does the pattern of transactions or activities on the account over time make sense?

Note: Enquiries to check whether complex or unusual transactions or structures have legitimate economic or lawful purpose or were conducted properly and in good faith are not regarded as Tipping Off.

7.2 Detection and On-going Monitoring by Team Members

All team members are responsible for the detection of ML/TF/PF based on a consideration of suspicious indicators/red flags and typologies. Examples of standard suspicious indicators/red flags and typologies for each business line would be highlighted in the country specific AML/CTF/CPF manual. It is important to note that the existence of a single suspicious indicator/red flag may on its own seem insufficient, but when combined with other indicators, the same should be discussed with or reported to the Responsible Officer.

Team members who manage the client relationship or accept and process client transactions, are the first line of defence in understanding the normal and expected activity of a client and are therefore in the best position to monitor transactions. These team members have certain specific responsibilities with regard to the ongoing transaction and client monitoring as follows:

i. Maintaining vigilance in the normal course of business to identify and escalate unusual or suspicious activity related to ML/TF/PF to the Responsible Officer in accordance with established reporting procedures at the Financial Subsidiary;
ii. Interacting with clients to update any CDD information or documentation as part of on-going reviews/updates as prescribed in the Client and Account Management Guidelines for the client's risk profile, and in any event, regardless of risk profile:
    a. Each time there is a material change in the client's information (e.g. change of employment, marital status, address, expired identification, etc.);
    b. When there is a one-off transaction or a series of transactions which appear unusual in the context of the client's known account behaviour;
    c. As needed, when a new party is added to an existing account or in the case of reactivation of an account;
    d. When there is suspicion of ML/TF/PF; and
    e. When there is doubt about the veracity or adequacy of previously obtained client identification data.
iii. Monitoring of client transactions over the life of the client relationship, and with particular reference to new accounts, closely scrutinising transactions within the first 6 months of the account being opened.

All team members must be vigilant in identifying changes in client transactions that appear inconsistent with the expected transaction type and activity level for the client. Where such a change in activity level is identified, the team member must communicate with the client and obtain up-to-date information including any expected change in profile or activity level. Such information should be documented and filed. If the team member believes the particular transaction or trend is unusual based on the understanding of the client, such a transaction should be reported immediately to the Compliance Department in keeping with the applicable internal reporting procedures.

7.3 Monitoring and Testing by the Compliance Team

Automated monitoring systems and manual reporting programmes managed by the Compliance Team are used to detect possible ML/TF/PF activity within the Financial Subsidiaries. Any alerts created or internal reports raised by the business are investigated and may result in reports being made to the Designated Authority, where applicable. An investigation may also be prompted based on information received from a team member or a Law Enforcement Agency, whether related or un-related to ML/TF/PF.

In relation to the monitoring of transactions, the Compliance Department is responsible for the following:

i. Daily monitoring of transactions and performing historical analyses of client accounts or transactions where necessary;
ii. Ensuring the names of new and existing clients are automatically compared to the most recent UN Consolidated List and any other applicable list;
iii. Conducting as required, due diligence and EDD reviews on clients including potential high-risk clients before a relationship is established;
iv. Updating the internal Watch List on an ongoing basis;

v. Working closely with the Regulators and Designated Authority and keeping abreast of international media in order to identify persons associated with illegal activity, Non-Cooperative countries, (specified jurisdictions) countries with weak AML/CTF/CPF frameworks and individuals and organisations associated with terrorism;
vi. Adopting a consolidated approach in the assessment of clients with multiple accounts within the FHL. These are to be reviewed periodically.
vii. Conducting compliance testing of aspects of the KYC Compliance Plan at each Branch and relevant business unit at least on an annual basis.

8. Prohibitions

The FHL Group upholds a prohibition on entering into relationships or performing transactions involving:

i. Anonymous accounts or accounts in fictitious names: the FHL, its subsidiaries and their branches will not open numbered/anonymous accounts or conduct transactions with persons by means of any such accounts;
ii. Shell banks ('shell bank' means a bank which has 'no physical presence' in the country in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision; and "physical presence" means that a meaningful mind and management is located within the same country);
iii. Internet casinos or companies involved in other forms of on-line gambling;
iv. Any business registered for the purposes of betting or gambling and entities registered as gaming houses or pool betting establishments (except as specifically approved by the Board of Directors of the Financial Subsidiary);
v. Adult websites;
vi. Companies involved in the on-line sale of pharmaceuticals;
vii. High Risk Jurisdictions subject to call for action by FATF or any other jurisdiction specified by the FHL Group or the relevant authorities from time to time;
viii. Designated Persons and Entities;
ix. Companies whose ownership structure is via Bearer Shares. Bearer Shares are shares which are owned by the persons holding these shares. This allows ownership of shares to change easily and it may be difficult to determine the true beneficial owner;
x. Foreign companies having nominee shareholders.
xi. Virtual or crypto currencies

There is also a general prohibition on transacting where:

i. Illegal activities are suspected: Clients whose information indicates possible involvement in illegal activities or the commission of a Predicate Offence.
ii. Proper verification is not possible: Clients with businesses that make it impossible to verify the legitimacy of their activities or the source of funds.
iii. A client refuses to provide information or documentation required for account opening or on-going due diligence.

9. Confidentiality

Any reports from the FHL and its Financial Subsidiaries and their branches which are submitted to the Designated Authority and any other regulatory body whether local or international pertaining to ML/TF/PF must remain confidential. Reports filed with the Designated Authority related to suspicious activity or transactions are to be kept confidential unless required to be disclosed a by court order or as required under the legal and regulatory framework.

Team members are therefore cautioned against disclosing to other team members, colleagues or clients that a report has been filed or that the transaction is, or appears to be suspicious or unusual, or is being investigated.

Team members will not be held liable in relation to any criminal, civil or administrative liability, as the case may be, for breach of any restriction on disclosure imposed by contract or any legislative, regulatory or administrative provision, if transactions are reported in accordance with this FHL policy and confidentiality of the report is maintained.

A team member who makes unauthorised disclosures of any confidential reports in relation to suspicious, unusual or threshold transactions or any other such regulatory report is subject to disciplinary action, including dismissal, and may also be subject to fines or prosecution under the legal and regulatory framework.

10. Training

Training programmes must be established to make all team members (including the team leaders) and Directors of the FHL and its Financial Subsidiaries, aware of their obligations in relation to matters of ML/TF/PF. These programmes should ensure there is a clear understanding of:

i. How the Financial Subsidiary might be used for ML/TF/PF to enable them to recognize and handle/report potential ML/TF/PF transactions and be aware of new techniques and trends in ML/TF/PF;
ii. Techniques for identifying and reporting unusual and suspicious transactions or activities;
iii. New developments and trends in AML/CTF/CPF including technological developments, where applicable;
iv. Actions to take once the risk is identified;
v. What the team member or the Director's role is in compliance efforts and how to perform that role;
vi. This Policy and its supporting procedures;
vii. The legal and regulatory framework for AML/CTF/CPF and their obligations thereunder;
viii. Disciplinary consequences for non-compliance.

In keeping with the record retention requirements in each jurisdiction, records must be maintained by the Responsible Officer on the persons trained, the dates of training, the subject matter of the training and the results of any testing carried out to measure understanding of the AML/CTF/CPF requirements. Refresher training will be provided at regular intervals, no less frequently than once per year.

All new hires will receive AML/CTF / CFP training as scheduled by Culture and Human Development Team (CHDT), and should take place prior to commencement of client facing/relevant activities. Training may take the form of in-person/classroom training, online training modules, videotaped presentations, intranet learning applications, compliance bulletins and other media-based training.

Each team member will be tested on the material and a pass rate of 80% must be achieved before certification is received. Where team members do not achieve the required 80% pass rate, a special training session will be held for such team members. They will be required to retake the assessment after the special training session.

11. Independent Reviews

The AML/CTF/CPF risk management framework of each Financial Subsidiary shall be reviewed by internal auditors and external auditors at the frequency prescribed in each jurisdiction. A report comprising their findings and recommendation shall be submitted to the Board of the Directors of the Financial Subsidiary by both the internal and external auditors and to the Regulators as prescribed in each jurisdiction.

In terms of scope, the external auditors are required to evaluate this Policy's adherence to applicable laws and regulations and the effectiveness of measures taken by FHL in implementing same.

Internal Audit is required to evaluate the adequacy of implementation of this Policy and the supporting procedures and systems, and the level of compliance with same. The review process should identify weaknesses in policies and procedures, corrective measures to be undertaken and Internal Audit should ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor and the Regulators have been satisfactorily addressed. Internal Audit should also review the Risk Assessment conducted under Section 5 hereof to ensure that it is sufficiently comprehensive.

Internal Audit's review should include inter alia:

i. A review of the Financial Subsidiary's risk assessment and risk rating process for reasonableness given its risk profile (products/services customers, geographic locations);
ii. A review of the adequacy of the ML/TF/PF risk assessment framework and application of a risk-based approach in the design of related controls;
iii. Appropriate risk-based transaction testing to verify adherence to this Policy and supporting procedures;
iv. An evaluation of management's efforts to resolve breaches and deficiencies noted in previous audits and regulatory examinations, including progress made in addressing outstanding regulatory actions, if applicable;
v. A review of training programs for effectiveness, completeness and frequency;

vi. A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for AML/CTF/CPF compliance including a review of the criteria and processes for identifying and reporting unusual and suspicious activities and transactions;
vii. An assessment of the overall process for identifying and reporting suspicious activity, including a review of 'not filed' (closed/not suspicious) internal suspicious transactions/activity reports to determine the adequacy, completeness and effectiveness of the adjudication process. It should be noted that the internal audit review does not include a review of actual Suspicious Activity Report (SAR)/ Suspicious Transaction Report (STR) filed with the FIU.

Finally, the Internal Audit review should include interviews with key team members, such as members of the Compliance Team, client-facing team members handling transactions and their supervisors, to determine their knowledge of the AML/CTF/CPF requirements, this Policy and supporting procedures.

12. Continuous Improvement and Testing

The Compliance Team has the responsibility for ongoing monitoring of the completion of all AML/CTF/CPF duties by the first line of defence. This includes assessments of AML/CTF/CPF compliance, review of exception reports, and reporting of significant compliance failures to the Board and/or the team leaders.

These assessments should be risk-based and constructed to validate that key assumptions, data sources and procedures used in measuring and monitoring AML/CTF/CPF compliance risks can be relied upon on an ongoing basis.

As part of the continuous improvement programme, robust AML/CTF/CPF compliance assessments play a key role in self-identifying weaknesses in existing AML/CTF/CPF controls and remediating identified deficiencies, and thus are essential to sustaining effective AML/CTF risk management. These assessments should therefore be included in the workplans of each Financial Subsidiary.

13. Policy Review

This FHL Policy shall be reviewed and updated by the GCCO or designate on an annual basis, or at such shorter intervals as may be necessary as events occur.

14. Policy Compliance

The Directors, team leaders, team members and other relevant stakeholders of the FHL and its Financial Subsidiaries are committed to comply with all the policies outlined in this document. Non-compliance will be taken seriously and may lead to disciplinary action.

15. Exceptions

Any exceptions to this policy must be approved by the FHL Board of Directors or a committee designated by them. Requests for exceptions must be documented and justified based on business needs and risks. Approved exceptions will be reviewed regularly to ensure they remain appropriate and acceptable.

16. Appendix

16.1. Governance Roles And Responsibilities

The Board of Directors of FHL

As noted prior, the Board of Directors of FHL has ownership of this Policy and has delegated responsibility for the oversight of AML/CTF/CPF matters to the Board of Directors of the Financial Subsidiaries. As such, they are responsible for:

i. Ensuring the establishment of an appropriate AML/CTF/CPF risk management framework comprising this Policy and any other policies that enable the FHL to manage and mitigate effectively its AML/CTF/CPF across the FHL Group;
ii. Approving this Policy and any amendments thereto;
iii. Appointing a GCCO with all attendant duties and responsibilities as set out in regulation and herein;
iv. Ensuring that the Group's People Policies adequately captures disciplinary action for non-compliance with regulatory requirements;
v. Ensuring the establishment and approval of an annual Enterprise Compliance Plan;
vi. Ensuring receipt of timely and comprehensive reports on the AML/CTF/CPF risks from the GCCO, including but not limited to:
    a. Remedial action plans, if any, to address the results of independent audits (either internal or external);
    b. Reports received from the regulators on its assessment of the AML/CTF/CPF compliance;
    c. Results of compliance testing and self-identified instances of non-compliance with AML/CTF/CPF requirements;
    d. Developments in AML/CTF/CPF laws and regulations and implications if any, to the Group;
    e. Details of recent significant risk events and potential impact on the Group;
    f. Metrics, including, but not limited to, statutory reporting, orders from law enforcement agencies, refused or declined business and de-risked relationship.
vii. Ensuring and seeking confirmation that each member of the Board of Directors of the FHL and its Financial Subsidiaries receives the requisite training on AML/CTF/CPF generally as well as on the FHL's specific AML/CTF/CPF risks and controls.

The Board of Directors of a Financial Subsidiary

Each Board of Directors of a Financial Subsidiary shall in its mandate outline details of its responsibilities related to AML/CTF/CPF compliance.

Each Board of Directors of a Financial Subsidiary is responsible for:

i. Ensuring the adoption of this Policy and that all policies, controls and procedures are in place to enable the Financial Subsidiary to effectively manage and mitigate its AML/CTF/CPF risks;
ii. Appointing a Responsible Officer with all attendant duties and responsibilities as set out in regulation and herein;
iii. Ensuring the establishment and approval of an annual Compliance Plan;
iv. Ensuring receipt of timely and comprehensive reports on the AML/CTF/CPF risks from the Responsible Officer including but not limited to:
    a. Remedial action plans if any, to address the results of independent audits (either internal or external);
    b. Reports received from the regulators on its assessment of the AML/CTF/CPF compliance;

c. Results of compliance testing and self-identified instances of non-compliance with AML/CTF/CPF requirements;
d. Developments in AML/CTF/CPF laws and regulations and implications if any, to the Financial Subsidiary;
e. Details of recent significant risk events and potential impact on the financial subsidiary;
f. Metrics including, but not limited to, statutory reporting, orders from law enforcement agencies, refused or declined business and de-risked relationships.

v. Ensuring and seeking confirmation that each member of the Board of Directors of a Financial Subsidiary receives the requisite training on AML/CTF/CPF generally as well as on FHL's specific AML/CTF/CPF risks and controls.

The Board Audit and Compliance Committee

Each Board Audit and Compliance Committee (BACC) shall in its mandate outline details of its responsibilities related to AML/CTF/CPF compliance. The Board of Directors of FHL has agreed to delegate its oversight of AML/CTF/CPF compliance to the Board of each Financial Subsidiary, who in turn has delegated the authority to its BACC (wherever one exists).

As such, each BACC is responsible for:

i. Reviewing and recommending proposed amendments to this Policy before they are submitted to its Board of Directors for approval/ratification;
ii. Reviewing internal and external audit reports on AML/CTF/CPF;
iii. Monitoring on-going AML/CTF/CPF activities and issues by reviewing reports prepared by the Responsible Officer or the Country Compliance Officer (CCO), RGO or GCCO, where applicable, on key developments and the state of AML/CTF/CPF compliance, and making appropriate recommendations in respect thereof;
iv. Reviewing the results of examinations by the regulators, compliance reviews, audits and other independent testing, as well as corrective actions planned or taken in response thereto; and
v. Updating the Board of Directors of the Financial Subsidiaries on the activities of the BACC.

The Group Chief Compliance Officer

The details of the functions of the GCCO are contained in the job scope for this role. The GCCO is primarily responsible for:

i. Designing and coordinating the implementation of a single AML/CTF/CPF strategy across the Group. This includes the implementation of mandatory policies and procedures where applicable;
ii. Ensuring that each financial subsidiary adopts this Policy, and that compliance metrics are established to measure adherence to same;
iii. Ensuring that the Board of Directors and the team leaders of FHL are kept up to date on current legislative requirements both locally and internationally;
iv. Reporting to the Board of Directors of FHL on: i) the adequacy of the AML/CTF/CPF risk management programme; ii) concerns with and recommendations for high risk relationships; and iii) any issues and material changes with remedial actions and milestones; adequacy of resources;
v. Producing reports on the execution of and compliance with the AML/CTF/CPF strategy including an annual comprehensive report to the Board of Directors and team leaders of FHL;
vi. Ensuring that the Compliance Teams across the Group are adequately resourced and receive appropriate and specialised annual training which allows them to execute their functions effectively;
vii. Acting as a liaison between the FHL and regulatory and law enforcement agencies, as well as external counsel, as needed, with respect to all compliance matters and investigations occurring in Jamaica;
viii. Maintaining oversight of significant recommendations made by internal and external auditors and the regulators, in respect of AML/CTF/CPF and ensuring that they are acted upon by the Compliance Team and team leaders in a timely manner;

ix. Making recommendations to ensure that the Compliance Team is resourced adequately in terms of people, Information Technology and monitoring systems, and budget to implement, administer and monitor AML/CTF/CPF compliance appropriately; and
x. Coordinating with the Internal Audit and Legal departments as required on AML/CTF/CPF matters and investigations, and on matters pertaining to targeted financial sanctions notified by the United Nations Security Council.

The GCCO is supported by, and authorised to assign any of their duties to, the Regional Governance Officer (RGO).

The Regional Governance Officer

The details of the functions of the RGO are contained in the job scope for this role. The RGO is primarily responsible for:

i. Overseeing the implementation by the CCO/Responsible Officer roles outlined in this Policy for territories in which the Group operates;
ii. Ensuring consolidated reporting to the GCCO on all aspects of the FHL Group's AML/CTF/CPF compliance activities;
iii. Coordinating the conduct of AML/CTF/CPF Risk Assessments for the FHL Group at least once every three years;
iv. Seeking assurance from the Responsible Officers that:
    a. Financial Subsidiaries are complying with the appropriate standards and procedures in place for AML/CTF/CPF;
    b. Training of all team members is being conducted at least annually and in accordance with applicable legal and regulatory requirements;
    c. Appropriate procedures and processes are in place at the Financial Subsidiary level for the detection and reporting of ML/TF/PF, internally and externally;
    d. A reporting system is in place whereby team members can report activities which are not in compliance with FHL's AML/CTF/CPF policies and procedures without fear of reprisal.
v. Ensuring the development and implementation of training programmes for AML/CTF/CPF across the Group in conjunction with the CCO/Responsible Officer and the Culture and Human Development Team;
vi. Ensuring that a compliance risk assessment is conducted as part of the business development process for all new products and services being contemplated by the FHL; and
vii. Supervising the activities of compliance function staff, including the CCO/Responsible Officer where applicable and providing feedback to them on observed emerging typologies, trends and risk across the FHL Group.

The RGO is supported by, and authorised to assign any of their duties to, the CCO. Where there is no RGO, the responsibilities will be assumed by the CCO.

The Country Compliance Officer

The details of the functions of the CCO are contained in the job scope for this role.

Where there is a CCO, the CCO will be responsible for:

i. Ensuring that there is a single strategy implemented across the country which aligns with the overarching FHL Group strategy for AML/CTF/CPF;
ii. Ensuring that the annual review of this FHL Policy by the Board of Directors of FHL is ratified at the Financial Subsidiary level, and that proper records are maintained of these reviews and any amendments made;
iii. Ensuring that the necessary procedures and controls required to support this FHL Policy are in place at the country level, where appropriate;
iv. Preparing monthly or bi-monthly reports to the RGO/GCCO on key developments and the state of AML/CTF/CPF compliance in the country;

v. Maintaining a register of all training administered to the Directors, team leaders and team members of the FHL and its Financial Subsidiaries on an annual basis;
vi. Reporting to the Financial Subsidiaries' Boards as needed on: i) concerns and recommendations for high risk relationships: ii) any issues and material changes, remedial actions and milestones: and iii) adequacy of resources to support the execution of this FHL Policy and its supporting procedures ;
vii. Making recommendations to the RGO for the updating of this FHL Policy;
viii. Providing feedback to Responsible Officers of any observed emerging typologies, trends and risk across the country.

The CCO is supported by, and authorised to assign any of their duties to, the Responsible Officer. Where there is no CCO, the responsibilities will be assumed by the Responsible Officer.

The Responsible Officer

As noted prior, the term "Responsible Officer" is used in this policy to describe the officer in charge of, or appointed with ultimate responsibility for AML/CTF/CPF compliance in a Financial Subsidiary. Depending on the jurisdiction, the name of this role may vary.

The details of the functions of the Responsible Officer are contained in the job scope for that role as described by jurisdiction. Responsible Officers are at a high level responsible for:

i. Overseeing AML/CTF/CPF control activity in all relevant business areas for the purpose of establishing a reasonable threshold level of control consistency throughout the Financial Subsidiary;
ii. Evaluating laws, guidance notes and regulations with the guidance of internal and external counsel where appropriate, to determine their applicability to the Financial Subsidiary;
iii. Ensuring that this FHL Policy is implemented, and necessary procedures and controls required to support this Policy are in place at the Financial Subsidiary in order to ensure that the AML/CTF/CPF framework is current with respect to the Financial Subsidiary's identified inherent risks and giving consideration to local developments in ML/TF/PF;
iv. Conducting risk assessments and timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF/PF risks and developing appropriate control mechanisms;
v. Conducting periodic assessments of AML/CTF/CPF control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF/PF risks, and assessing operational changes including the introduction of new technology and processes to ensure that ML/TF/PF risks are addressed;
vi. Ensuring that systems and processes that generate information used in reports to team leaders and the Board of Directors are adequate and appropriate, and that they use consistent reporting criteria and generate accurate information;
vii. Advising all relevant internal personnel in the Financial Subsidiary and branches of the Financial Actions Task Force's (FATF) and the Caribbean Financial Action Task Force (CFATF) listing of jurisdictions with deficiencies in their AML/CTF/CPF regimes, and any periodic updates thereto (Specified Jurisdictions);
viii. Co-operating with and acting as the liaison officer to local regulators and law enforcement agencies with respect to all compliance matters and investigations;
ix. Maintaining records of all suspicious/unusual transactions reports received and all reports forwarded to external regulatory and reporting bodies;
x. Evaluating reports of suspicious/unusual transactions from team members and ensuring that reports for Threshold reporting (where applicable), Suspicious Activity and Suspicious Transactions are submitted to external regulatory and reporting bodies in a timely manner;
xi. Ensuring that appropriate training is administered with respect to AML/CTF/CPF to all team members of the Financial Subsidiary as scheduled by CHDT for new hires, and thereafter on an annual basis, and maintaining a team member training register;
xii. Preparing periodic reports to the Financial Subsidiary's BACC on key developments and the state of AML/CTF/CPF compliance in the Financial Subsidiary, including:

a. Significant regulatory changes;
b. Regulatory examination and internal audit results;
c. Risk assessments;
d. Statistical data on high-risk accounts;
e. Filings with the Designated Authority, including trends;
f. Potential issues and backlogs;
g. Training schedule and completion ratio;
h. Staffing levels versus staffing plan;
i. Key leadership/staffing shortages in critical compliance and operations departments;
j. Potential impact of new products and service offerings in the pipeline;

xiii. Advising the Board of Directors of the Financial Subsidiary, through its BACC, independently, of any material compliance and/or regulatory risk posed to the entity.

The Compliance Team

The Compliance Teams acts as a partner and advisor to the business and support units in implementing and executing on this FHL Policy and its supporting procedures. The details of the functions of the Analysts in the Compliance Team are contained in the job scope for that role as described in the jurisdiction. Their primary responsibilities include:

i. Supporting the Responsible Officer in the execution of their functions;
ii. Monitoring of client accounts as prescribed;
iii. Identifying, monitoring and investigating any potentially suspicious activities highlighted by monitoring systems and referred by business units, and making the appropriate reports to the Responsible Officer;
iv. Providing guidance to business units on the proper application and interpretation of laws, regulations and policies applicable to AML/CTF/CPF and to new products, services and delivery channels;
v. Administering appropriate training and awareness programmes and communications as directed by the Responsible Officer;
vi. Reviewing, as prescribed, clients requiring EDD, including those classified as High Risk;
vii. Advising on EDD or where applicable, recommending approval of business relationships and transactions with any client resident or domiciled in a Specified Jurisdiction or any company that is incorporated in a Specified Jurisdiction;
viii. Conducting routine and targeted compliance testing of the business units' related AML/CTF/CPF procedures and of other key units with AML/CTF/CPF responsibilities.

Team Leaders

Team leaders, in collaboration with the Compliance Team, are responsible for the day-to-day implementation, monitoring and management of the Compliance Plan, including ensuring adherence to same.

Team Leaders are responsible for ensuring that:

i. The procedures that are in place to manage AML/CTF/CPF risk are consistent with the Financial Subsidiary's business model, product and service offerings, and risk appetite. To that end, team leaders must ensure that attention is paid to new and developing technologies and that there is an assessment of the ML/TF/PF risks arising from new products/services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks.
ii. Risk assessments take place prior to the launch of new products/services, channels and business practices and technologies.
iii. Significant recommendations made by internal and external auditors and regulators in respect of AML/CTF/CPF are acted upon in a timely manner;
iv. A strong culture of compliance is inculcated in each Financial Subsidiary, business unit and branch and that each business unit and branch takes ownership of and is accountable for implementing

this FHL Policy and its supporting procedures, and that corrective action is taken when breaches are identified;

v. The Compliance Team has unfettered access to information and personnel as required for the conduct of their duties.
vi. Controls are in place to monitor that detection and reporting procedures are being followed, and these should include:
    a. Clear lines of authority and responsibility;
    b. Segregation of duties;
    c. Job rotation;
    d. Establishment of designated limits; and
    e. Identification and monitoring of key risks.

The Culture and Human Development Team

The Culture and Human Development Team (CHDT) is responsible for:

i. Working with all business units to determine how best to incorporate compliance with this FHL Policy in performance evaluations and incentives;
ii. Implementing a comprehensive on-boarding screening process for all new hires, and on an on-going, risk-based basis;
iii. Working with the Compliance Teams to ensure that all team members receive annual training;
iv. Ensuring that on recruitment all new team members receive AML/CTF/CPF training;
v. Applying disciplinary action as may be necessary when team members fail to comply with this FHL Policy and its supporting procedures.

All Team Members

All team members must comply with this FHL Policy and its supporting procedures. In addition, team members must:

i. Maintain vigilance in the normal course of business to identify and escalate suspected ML/TF/PF activity to the Responsible Officer in accordance with established reporting procedures at the Financial Subsidiary;
ii. Participate in targeted AML/CTF/CPF training on an annual basis, or at such shorter interval as may be necessary.

16.2. Applicable Legal and Regulatory Framework

The below legal and regulatory frameworks are to be used by each jurisdiction in the development of their detailed AML/CTF/CPF manuals.

International Standards

- Basel Committee on Banking Supervision
- The USA Patriot Act
- The Foreign Narcotics Designation Kingpin Act and Regulations
- USA Economic Sanctions Programme
- The Financial Action Task Force on Money Laundering
- UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
- UN International Convention for the Suppression of the Financing of Terrorism
- UN Resolution 1373 on Threats to International Peace and Security caused by Terrorism

Jamaica

The following are the main aspects of the legal and regulatory framework in Jamaica governing ML/TF/PF:

- Proceeds of Crime Act, 2007 and 2013, 2016 & 2019 amendments
- Proceeds of Crime (Money Laundering Prevention) Regulations, 2007 and 2013 & 2019 amendments
- Terrorism Prevention Act, 2005 and 2011 & 2019 amendments
- The Terrorism Prevention (Reporting Entities) Regulation 2010 and 2019 amendment
- United National Security Council Resolutions Implementation Act, 2013 and 2019 amendment
- The United Nations Security Council Resolution Implementation (Reporting Entities) Regulations, 2019
- The United Nations Security Council Resolution Implementation (Asset Freeze – Democratic People's Republic of Korea) Regulations (DPRK Regulations) 2013;
- Guidance Notes issued by Supervisory/ Regulatory Authorities (BOJ & Financial Services Commission (FSC)

Trinidad and Tobago

The following are the main aspects of the legal and regulatory framework in Trinidad and Tobago governing ML/TF/PF:

- Proceeds of Crime Act, 2000 and the Regulations made thereunder
- Financial Obligation Regulations 2010
- Anti-Terrorism Act 2005 and the Regulations made thereunder
- Financial Intelligence Unit of Trinidad and Tobago Act 2009 and the Regulations made thereunder
- Economic Sanctions Act – Legal Notices No. 184 and 185 of 2018
- All relevant Guidelines issued by the Central Bank of Trinidad and Tobago (CBTT) and the Trinidad and Tobago Securities and Exchange Commission (TTSEC) pertaining to AML/CTF/CPF

Dominican Republic

The following are the main aspects of the legal and regulatory framework in Dominican Republic governing ML/TF/PF:

- Law 155-17 Anti-money Laundering and Terrorist Financing Act (2017)
- Decree No. 408-17 Application of Law 155-17
- Decree No.407-17 Application of Measures for the Preventive Freezing of Goods or Assets Related to Terrorism and its Financing
- Law 631-16 Asset Forfeiture (2016)
- Guidelines from the Financial Analysis Unit (UAF)
- Guidelines from the Superintendency of Banks
- Guidelines from the Central Bank of Dominican Republic
- Guidelines from the National Committee Against Money Laundering and Terrorist Financing
- Guidelines from the National Drug Council
- Guidelines from the Secretariat of Finance

Barbados

The following are the main aspects of the legal and regulatory framework in Barbados governing ML/TF/PF:

- The Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23
- The Money Laundering and Financing of Terrorism (Prevention and Control) Amendment Act, 2019 -22
- The Money Laundering (Prevention and Control) Act 1998
- Anti-Terrorism Act, 158A
- Anti-Terrorism (Amendment) Act, 2019
- Anti-Money/Combating Terrorist Financing Guideline for Financial Institutions Licensed Under the Financial Institutions Act, 324A and the International Financial Services Act Cap. 325
- Proceeds and Instrumentalities of Crime Act, 2019-4
- Mutual Assistance in Criminal Matters Act, Cap.140A
- Guidelines from the Central Bank of Barbados
- Guidelines from the Financial Services Commission
- Guidelines from The International Business Unit (IBU) of the Ministry of International Business and Industry
- Guidelines from the Barbados Financial Intelligence Unit

16.3. Document Change History

1. Entire document

Version #	Date	Change Description
1.0	August 24, 2023 (BACC) September 28, 2023 (BOD)	Comprehensive update